Integrating Microsoft Windows DFS

EventTracker Enterprise
Abstract

The purpose of this document is to help users in monitoring Microsoft Windows DFS by deploying Windows Agent.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and Microsoft Windows Server 2003 and later.

Intended audience

Administrators, who are assigned the task to monitor and manage Microsoft Windows Server 2003 and later events, using EventTracker.
Table of Contents

Abstract.................................................................................................................................................. 1
Scope..................................................................................................................................................... 1
  Intended audience ............................................................................................................................. 1
Pre-requisite.......................................................................................................................................... 3
Enable audit local group policy for DFS................................................................................................. 3
EventTracker Agent configuration ........................................................................................................ 6
EventTracker Knowledge Pack (KP)....................................................................................................... 9
  Categories .......................................................................................................................................... 9
  Reports ............................................................................................................................................... 9
  Alerts ................................................................................................................................................ 10
  Dashboards ...................................................................................................................................... 10
Import knowledge pack into EventTracker .............................................................................................. 11
  To import Alerts ............................................................................................................................... 12
  To import Category .......................................................................................................................... 13
  To import Tokens ............................................................................................................................. 14
  To import Flex Reports .................................................................................................................... 15
  To Configure Flex Dashboard ........................................................................................................... 16
Verify knowledge pack in EventTracker .............................................................................................. 20
  Verify Alerts ..................................................................................................................................... 20
  Verify Categories ............................................................................................................................ 21
  Verify Tokens .................................................................................................................................. 22
  Verify Flex Reports .......................................................................................................................... 23
Sample Reports ................................................................................................................................... 24
Sample Dashboards............................................................................................................................... 25
Overview

Distributed File System (DFS) is a set of client and server services that allow an organization, using Microsoft Windows servers, to organize many distributed SMB file shares into a distributed file system.

Distributed File System is implemented as a role service of the File Services role. Distributed File System consists of two role services:

- DFS Namespaces
- DFS Replication

Pre-requisite

Prior to configuring Windows Server 2003 and later and EventTracker 7.x and later, ensure that you meet the following prerequisites:

- Administrative access on EventTracker.
- User should have Administrative rights on Microsoft Windows DFS.

Enable audit local group policy for DFS

1. Run `gpedit.msc`
2. Open the Group Policy Editor.
4. Expand this node, go to Object Access (Audit Policies->Object Access), then select the setting Audit Detailed File Share Audit, Audit File Share, Audit File System.
5. Select **Audit Detailed File Share**, right click and select **Properties**. In **Properties** console enable the check box to configure the following audit events: **Success** and **Failure**.
6. Repeat Step 5 for Audit File Share and Audit File System.
EventTracker Agent configuration

1. Deploy EventTracker Agent in Microsoft Windows Distributed File Services Server, please follow the steps mentioned in How to Install EventTracker and Change Audit.

2. Select the Start > All Programs > Prism Microsystems > EventTracker.

3. In EventTracker Control Panel, and select EventTracker Agent Configuration.

4. Select Event Filters tab, and then click the Filter Exception button.
Filter Exception window displays.

5. Click the **New** button.

![Figure 4](image-url)

Event Details window displays.

6. In **Match in Source** box, enter *‘Microsoft-Windows-Security-Auditing’* and specify **Event ID:** 5140.

![Figure 5](image-url)
7. Click the **OK** button.
8. **Save** the configuration and **Close** the EventTracker Agent Configuration window.
EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Categories, reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Distributed File System.

Categories

- **Microsoft Windows DFS: User logon** - This category based report provides information related to users whose account was successfully logged on.

- **Microsoft Windows DFS: Network share object accessed** - This category based report provides information related to account details, network information, shared path details and related accesses.

- **Microsoft Windows DFS: Auditing setting changed** - This category based report provides information related to when admin change the audit SACL of an object, such as file or folder auditing settings on object were changed.

- **Microsoft Windows DFS: Client desired access** - This category based report provides information related to a network share object that was checked to see whether client can be granted desired access or not granted.

- **Microsoft Windows DFS: Namespace activity** – This category based report provides information related to whether DFS has connected to active directory or facing any issues while connecting and also whether server has finished initialization of building namespaces.

- **Microsoft Windows DFS: Replication activity** – This category based report provides information related to replication initialization, replicated folder information and replicated folder violation details.

Reports

- **Microsoft Windows DFS: User logon** - This report provides information related to DFS login which includes columns such as account name, account domain, logon type, source address, source port and workstation name.
• **Microsoft Windows DFS: Network share object accessed** - This report provides information related to network share object accessed which includes columns such as account name, account domain, object type, source address, source port, share name, share path and accesses.

• **Microsoft Windows DFS: Auditing setting changed** - This report provides information related to auditing setting changed which includes columns such as account name, account domain, object server, object type, object name and new security descriptor details.

• **Microsoft Windows DFS: Client desired access** - This report provides information related to client desired access which includes columns such as account name, account domain, object type, source address, source port, share name, share path, relative target name, access request information and access check results and whether desired access is granted or not granted.

• **Microsoft Windows DFS: Namespace activity** - This report provides information related to namespace activity which includes shared folder details located at dfsroots.

• **Microsoft Windows DFS: Replication activity** – This report provides information related replication activity which includes replicated folder root, file path, replicated folder name and replicated group name.

**Alerts**

• **Microsoft Windows DFS: Namespace active directory issues** - This alert is generated when DFS server fails to contact domain controller, active directory and unable to access private data from active directory.

• **Microsoft Windows DFS: Replication stopped** - This alert is generated when DFS replication service stops replication on the replicated folder.

**Dashboards**

• **Microsoft Windows DFS: User logon** – This dashboard give us the information about users, whose account was successfully logged on.
Import knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**. Click **Import** tab.

![EventTracker Control Panel](image)

Figure 7

Import **Alerts/Category/Tokens/ Flex Reports** as given below.
To import Alerts

1. Click **Alerts** option, and then click the **browse** button.

![Export Import Utility](image8.png)

Figure 8

2. Locate **Microsoft Windows DFS.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.

EventTracker displays success message.

![Export Import Utility](image9.png)

Figure 9
4. Click OK, and then click the Close button.

To import Category

1. Click Category option, and then click the browse button.

![Export Import Utility](image)

Figure 10

2. Locate Microsoft Windows DFS.iscat file, and then click the Open button.

3. To import categories, click the Import button.

   EventTracker displays success message.

![Export Import Utility](image)

Figure 11
4. Click **OK**, and then click the **Close** button.

**To import Tokens**

1. Click **Token value** option, and then click the browse button.

![Figure 12](image)

2. Locate the **Microsoft Windows DFS.istoken** file, and then click the **Open** button.

3. To import tokens, click the **Import** button.

EventTracker displays success message.

![Figure 13](image)
4. Click **OK**, and then click the **Close** button.

To import Flex Reports

1. Click **Report** option, and then click the browse button.

![Screen shot of Export Import Utility](image1)

**Figure 14**

2. Locate the **Microsoft Windows DFS.issch** file, and then click the **Open** button.

3. Click the **Import** button to import the scheduled reports.

EventTracker displays success message.

![Screen shot of Export Import Utility](image2)

**Figure 15**
4. Click the **OK** button. Click the **Close** button.

To Configure Flex Dashboard

1. Schedule flex reports (Microsoft Windows DFS: User logon) after importing them.
2. During scheduling, please check **Persist data in EventVault Explorer** and select all the columns to persist.

![REPORT WIZARD](image)

*Figure 16*
3. Now, wait for report to run as per schedule time or run it manually.
4. After generating report, click on Dashboard > Flex.
5. Click on Add Dashboard button and fill Title and Description box and save it.
6. Now, create Dashlet for Microsoft DNS (Top URL usage) by clicking on **Configure flex dashlet**.

7. Fill **WIDGET TITLE** (Top URL usage), select **DATA SOURCE** (Microsoft DNS-Name resolution successfully), select **CHART TYPE** and select **AXIS LABELS [X-AXIS]**.
8. After selecting and filling all the options, click on the **TEST** button to check the Dashlet. If data are coming properly, then click on **CONFIGURE** button.

![Figure 21](image1)

9. After creation of Dashlet for Microsoft Windows DFS User login, click on **Customize flex dashlet**.

10. Select Microsoft Windows DFS User login: Top URL usage dashlet and click on **ADD** button.

![Figure 22](image2)
11. Now, you can see the Dashlet on Dashboard.

Verify knowledge pack in EventTracker

Verify Alerts

1. Logon to EventTracker Enterprise.

2. Click Admin dropdown, and then click Alert

3. In Search field, type 'Microsoft Windows DFS', and then click the Go button.

   Alert Management page will display all the imported Microsoft Windows DFS alerts.
4. To activate the imported alerts, select the respective checkbox in the Active column.

EventTracker displays message box.

![Message from webpage](image)

**Figure 24**

5. Click OK, and then click the **Activate Now** button.

**NOTE:**

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

**Verify Categories**

1. Logon to **EventTracker Enterprise**.

2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree**, to view imported categories, scroll down and expand Microsoft Windows DFS group folder to view the imported categories.

![Figure 26](image)

**Verify Tokens**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rule**.

![Figure 27](image)
Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports.
3. Select the Configuration.
4. In the Reports Configuration, select Defined radio button.
   EventTracker displays Defined page.
5. In search box enter Microsoft Windows DFS.
   EventTracker displays flex reports of Microsoft Windows DFS.

![Figure 28](image-url)
Sample Reports

1) Microsoft Windows DFS: User logon

![Table: Microsoft Windows DFS-User logon]

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Account Name</th>
<th>Account Domain</th>
<th>Source Computer</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Logon Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/09/2016 07:14:52 PM</td>
<td>DFS-SERVER</td>
<td>Jackson</td>
<td>Contoso</td>
<td>mercury</td>
<td>192.168.11.72</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>01/09/2016 07:15:40 PM</td>
<td>DFS-SERVER</td>
<td>Stephen</td>
<td>Contoso</td>
<td>venus</td>
<td>192.168.11.96</td>
<td>51258</td>
<td>3</td>
</tr>
<tr>
<td>01/09/2016 07:16:43 PM</td>
<td>DFS-SERVER</td>
<td>William</td>
<td>Contoso</td>
<td>bacoce</td>
<td>192.168.11.33</td>
<td>41630</td>
<td>3</td>
</tr>
<tr>
<td>01/09/2016 07:17:56 PM</td>
<td>DFS-SERVER</td>
<td>Sophie</td>
<td>Contoso</td>
<td>cam</td>
<td>192.168.11.111</td>
<td>50459</td>
<td>3</td>
</tr>
<tr>
<td>01/09/2016 07:19:55 PM</td>
<td>DFS-SERVER</td>
<td>Thomas</td>
<td>Contoso</td>
<td>harry</td>
<td>192.168.11.150</td>
<td>51459</td>
<td>3</td>
</tr>
<tr>
<td>01/09/2016 07:22:40 PM</td>
<td>DFS-SERVER</td>
<td>Vinci</td>
<td>Contoso</td>
<td>moc</td>
<td>192.168.11.111</td>
<td>42559</td>
<td>3</td>
</tr>
<tr>
<td>01/09/2016 07:25:43 PM</td>
<td>DFS-SERVER</td>
<td>Junny</td>
<td>Contoso</td>
<td>plato</td>
<td>192.168.11.128</td>
<td>51385</td>
<td>3</td>
</tr>
<tr>
<td>01/09/2016 07:30:39 PM</td>
<td>DFS-SERVER</td>
<td>Leonard</td>
<td>Contoso</td>
<td>hui</td>
<td>192.168.11.161</td>
<td>51659</td>
<td>3</td>
</tr>
</tbody>
</table>

2) Microsoft Windows DFS-Auditing settings changed

![Table: Microsoft Windows DFS-Auditing settings changed]

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Account Name</th>
<th>Account Domain</th>
<th>Object Server</th>
<th>Object Type</th>
<th>Object Path</th>
<th>New Security Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/04/2016 05:16:45 PM</td>
<td>DFS-SERVER</td>
<td>ericadmin</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
<tr>
<td>01/04/2016 05:16:42 PM</td>
<td>DFS-SERVER</td>
<td>Amy</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
<tr>
<td>01/04/2016 05:20:45 PM</td>
<td>DFS-SERVER</td>
<td>Mike</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
<tr>
<td>01/04/2016 05:25:22 PM</td>
<td>DFS-SERVER</td>
<td>Michel</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
<tr>
<td>01/04/2016 05:35:45 PM</td>
<td>DFS-SERVER</td>
<td>Joseph</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
<tr>
<td>01/04/2016 05:40:42 PM</td>
<td>DFS-SERVER</td>
<td>Jack</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
<tr>
<td>01/04/2016 05:55:22 PM</td>
<td>DFS-SERVER</td>
<td>Jerry</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
<tr>
<td>01/04/2016 05:56:12 PM</td>
<td>DFS-SERVER</td>
<td>Henry</td>
<td>Contoso</td>
<td>Security</td>
<td>File</td>
<td>F:DFS\Root\perm</td>
<td>S:ARAI</td>
</tr>
</tbody>
</table>
Sample Dashboards

1. Microsoft Windows DFS- User logon

![Figure 31](image-url)